![NASA logo] National Aeronautics and Space Administration	# Information and Technology Classification and/or Sensitivity Level Determination Checklist

NASA OFFICE OF SECURITY AND PROGRAM PROTECTION
Program and Project Review Checklist for Possible Designation as Classified National Security Information (CNSI) or Sensitive But Unclassified (SBU) Information

PROGRAM/PROJECT TITLE

PROGRAM/PROJECT

A. REVIEW FOR CLASSIFIED NATIONAL SECURITY INFORMATION (CNSI)

Prior to conducting the below review, program/project evaluators should coordinate with the Center Office of Security for guidance and assistance during the assessment.

Will this program or project involve generation of or access to information, material, and or technology concerning: **YES**   **NO**

- Military plans, weapons systems, or operations? ☐ ☐

- Foreign government information? ☐ ☐

- Intelligence activities (including special activities), intelligence sources or methods, or cryptology? ☐ ☐

- Foreign relations or foreign activities of the United States, including confidential sources? ☐ ☐

- Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism? ☐ ☐

- United States Government programs for safeguarding nuclear materials or facilities? ☐ ☐

- Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism?, or ☐ ☐

- Weapons of mass destruction? ☐ ☐

- Ongoing research, the results of which could constitute "breakthrough" technologies that may have military applications or aid transnational terrorism? ☐ ☐

- Information and/or technology currently under a classification caveat applied by NASA, other government agencies, or industrial partner? ☐ ☐

If you answered **Yes** to any of the categories outlined above; information, material, and/or technology generated and/or accessed by this program or project requires a comprehensive review for designation as Classified National Security Information (CNSI) Program, and subsequent implementation of appropriate security and accountability measures, if required. Refer to Chapter 5, section 5.23, NPR 1600.1 for guidance.

When implemented through a contract, grant, cooperative agreement, or other binding agreement (MOA/MOA, etc.) it must undergo further review, per National Security Decision Directive (NSDD) 189 prior to its award.

You must coordinate with the Center Security Office for support in conducting the review under Executive Order 12958 and amended by Executive Order 13292, "Classified National Security Information," and subsequent development/issuance of a DD Form 254, "Department of Defense Contract Security Classification Specification," as appropriate.

If you answered **No** to the categories outlined above you **may not** designate any of the information and/or technology as classified national security information. Any changes in status from unclassified to classified information must be coordinated with the respective Center Security Office.

B. REVIEW FOR DESIGNATION AS SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION

Will this program or project involve access to or generation of: **YES**   **NO**

- Information exempted from disclosure by statute (e.g., Export Administration Regulations (EAR), International Traffic in Arms Regulation (ITAR), and Section 303(b) of the Space Act)? ☐ ☐

- Information and material originated within or furnished to NASA which falls under one or more of the exemption criteria of the Freedom of Information Act? ☐ ☐

- Geological and geophysical information and data, including maps, concerning wells? ☐ ☐

- Center maps and/or plain text documents describing locations and directions (e.g., latitude, longitude, depth, etc.) of underground utility conduits (e.g., sewers, gas, data, communications, etc.)? ☐ ☐

B. REVIEW FOR DESIGNATION AS SENSITIVE BUT UNCLASSIFIED (SBU) INFORMATION *(CONTINUED)*	**YES**	**NO**
• Drawings and specifications which identify mission essential infrastructure designated assets or other key resources?	☐	☐
• Mission and/or asset specific security plans that identify protective measures and procedures for assets that are sensitive but unclassified (SBU) in nature?	☐	☐
(Example: Payloads that utilize special nuclear materials, payloads that contain certain animal experiments, STS missions, communications assets, MEI assets, etc.)	☐	☐
• Emergency contingency or continuity of operations plans that provide detailed information regarding emergency response processes and procedures, including designation of relocation sites, that if publicized, could give a potential adversary vital information with which to thwart or compromise emergency response efforts?	☐	☐
NOTE: Under Department of Homeland Security guidelines, the identification of 3 or more relocation sites automatically requires classification of the document as Secret.		
• Information which is determined by a designated NASA official to be unusually sensitive (e.g., predecisional materials such as national space policy not yet publicly released, pending reorganization plans, or sensitive travel itineraries (refer to paragraph 5.24.5 for decontrol provisions))?	☐	☐
• Information, technologies or material determined by another agency for designation as sensitive but unclassified?	☐	☐
• Information that could be sold for profit?	☐	☐
• Information that could result in physical risk to personnel?	☐	☐
• NASA information technology (IT) internal systems data revealing infrastructure used for servers, desktops, and networks; applications name, version and release; switching, router, and gateway information; interconnections and access methods; mission or business use/need? Examples of information are systems inventories and enterprise architecture models.	☐	☐
• Systems security data revealing the security posture of the system? For example, threat assessments, system security plans, contingency plans, risk management plans, Business Impact Analysis studies, and Certification and Accreditation documentation.	☐	☐
• Reviews or reports illustrating or disclosing facility infrastructure or security vulnerabilities, whether to persons, systems, or facilities, not otherwise eligible for classification under Executive Order 12958, as amended?	☐	☐
• Information that could constitute an indicator of U.S. Government intentions, capabilities, operations, or activities or otherwise threaten operations security?	☐	☐
• Developing or current technology, the release of which could hinder the objectives of NASA, compromise a technological advantage or countermeasure, cause a denial of service, or provide an adversary with sufficient information to clone, counterfeit, or circumvent a process or system?	☐	☐

If you answered **Yes** to any of the categories above, appropriate protection and accountability measures must be implemented to ensure access is provided only to those authorized in the performance of their duties, including performance of a contract, grant, cooperative agreement, or other binding agreement. Foreign National access (including legal permanent resident aliens) will be based on a case-by-case assessment of the need and sensitivities of the information and technology. Refer to Chapter 5, Section 5.24, NPR 1600.1, and coordinate with the respective Center Security Office, Export Control Office, Freedom of Information (FOIA) Office, or Privacy Act Office, as appropriate, for protection, accountability, and/or release process and procedural requirements.

C. REVIEW FOR DESIGNATION AS NASA CRITICAL INFRASTRUCTURE OR KEY RESOURCE	**YES**	**NO**
Will this program or project involve the development and use of assets and/or facilities requiring designation as NASA Critical Infrastructure or Key Resources and subsequent inclusion under the NASA Mission Essential Infrastructure Protection Program (MEIPP)? Refer to NPR 1600.1, Chapter 8, Section 8.4, and Appendix H.	☐	☐

If you answered **Yes** to this question you must coordinate with Center Security and follow the requirements of NPR 1600.1.

PRINTED NAME AND TITLE OF EVALUATOR	SIGNATURE OF EVALUATOR	DATE
PRINTED NAME OF SECURITY OFFICE EVALUATOR	SIGNATURE OF SECURITY OFFICE EVALUATOR	DATE

NOTE: This completed and signed form must be included as part of the program/project documentation, as established in NPR 7120.5C, and attached to the file copy of any associated contract, grant or other binding agreement. A copy must be provided to the Center Security Office.